

Performance of the Fuzzy Vault for Multiple Fingerprints

(Extended Version)

Johannes Merkle, Matthias Niesing, Michael Schwaiger
secunet Security Networks AG
D-45128 Essen, Germany
johannes.merkle@secunet.com,
matthias.niesing@secunet.com
michael.schwaiger@secunet.com

Heinrich Ihmor, Ulrike Korte
Bundesamt für Sicherheit in der Informationstechnik
D-53175 Bonn, Germany
heinrich.ihmor@bsi.bund.de
ulrike.korte@bsi.bund.de

Abstract—The fuzzy vault is an error tolerant authentication method that ensures the privacy of the stored reference data. Several publications have proposed the application of the fuzzy vault to fingerprints, but the results of subsequent analyses indicate that a single finger does not contain sufficient information for a secure implementation.

In this contribution, we present an implementation of a fuzzy vault based on minutiae information in several fingerprints aiming at a security level comparable to current cryptographic applications. We analyze and empirically evaluate the security, efficiency, and robustness of the construction and several optimizations. The results allow an assessment of the capacity of the scheme and an appropriate selection of parameters. Finally, we report on a practical simulation conducted with ten users.

This article represents a full version of [1], copyright of Gesellschaft für Informatik (GI).

I. INTRODUCTION

Biometric authentication requires the storage of reference data for identity verification, either centrally (e.g., in a database) or locally (e.g., on the users token). However, the storage of biometric reference data poses considerable information security risks to the biometric application and concerns regarding data protection. As a potential solution to this dilemma, *biometric template protection* systems [2] use reference data which reveal only very limited information on the biometric trait. Another term frequently used for these schemes is *biometric encryption*. One of the most prominent approaches is the fuzzy vault scheme [3], where the sensitive information (the biometric reference data) is hidden among random *chaff points*.

In [4], [5], [6], [7], the application of the fuzzy vault scheme to minutiae (*fuzzy fingerprint vault*) has been proposed. However, a subsequent analysis in [8] has revealed that the parameters suggested do not provide security beyond 50 bit cryptographic keys. One of the suggestions in [8] was to enhance security by using multiple fingers. This idea is supported by the observation in [9] that a single fingerprint cannot provide enough entropy to

implement a secure biometric template protection. Further motivation for extending the fuzzy fingerprint vault to multiple fingers is provided by the analysis carried out in [10], which shows that the number of minutiae needed to obtain a provable secure scheme based on the results of [11] is much larger than the number of minutiae typically detected on a single fingerprint.

In this paper we present an implementation of a fuzzy vault based on the minutiae data of several fingerprints. We investigate the security, efficiency, and robustness of the scheme and of several optimizations applied, some of which have already been proposed in the previous constructions [4], [5], [6], [7]. In particular, we evaluate the impact of the basic parameters and optimizations to error rates, efficiency and security, and we derive suggestions for parameter selection. Furthermore, we evaluate the practical performance of the scheme in an experiment with 10 users.

This article is structured as follows: In Section II, we specify the fuzzy multi-fingerprint vault and its optimizations and justify our design decisions. Section III recapitulates existing security results and contains additional security analysis of optimizations applied. In Section IV, we report the results obtained in evaluation with real fingerprints. Finally, in Section V, we draw conclusions and identify open issues for future investigations.

II. DESIGN OF THE SCHEME

A. Basic biometric feature

We base our biometric feature vectors on minutiae. Since the minutiae orientations resemble the orientation of the ridges at the minutiae position, they bear strong dependencies with the minutia location and with the orientation of other minutiae. Although such dependencies are hard to quantify, they could be exploited by sophisticated attacks to effectively reduce the search space. Furthermore, in the fuzzy vault scheme the stored minutiae are hidden in a large set of chaff points which must be indistinguishable from real minutiae; this objective is much harder to achieve

if minutiae orientations are used as well. For these reasons we compose the feature vector of the minutiae location information (and the indexes of the corresponding fingers) only.

B. Underlying biometric template protection scheme

In the fuzzy vault scheme [3], a polynomial is used to redundantly encode a set of (pairwise distinct) private attributes m_1, \dots, m_t (e.g., biometric feature data) using a variant of Reed-Solomon decoding. First, a random (secret) polynomial $P(z)$ over a finite field \mathbf{F}_q with degree smaller than k is chosen. Then, each attribute m_i is encoded as element x_i of the finite field, i.e. $x_i = E(m_i)$, where E is an arbitrary injective map from the space of attributes to \mathbf{F}_q . Each of these elements x_i is evaluated over the polynomial, resulting in a list of (pairwise distinct) pairs $(x_i, y_i) \in \mathbf{F}_q^2$ with $y_i = P(x_i)$. In order to hide the private attributes, $r - t$ chaff points $x_{t+1}, \dots, x_r \in \mathbf{F}_q$ are randomly selected so that $x_i \neq x_j$ for all $1 \leq i < j \leq r$. For each chaff point x_i , a random $y_i \in \mathbf{F}_q$ with $y_i \neq P(x_i)$ is chosen. The list of all pairs $(x_1, y_1), \dots, (x_r, y_r)$, sorted in a predetermined order to conceal which points are genuine and which are the chaff points, is stored as the *vault*.

For authentication and recovery of the secret polynomial, another set of attributes (the query set) has to be presented. This set is compared with the stored fuzzy vault $(x_1, y_1), \dots, (x_r, y_r)$, and those pairs (x_i, y_i) are selected for which x_i corresponds to an attribute in the query set. The selected points are then used to try to recover the secret polynomial using Reed-Solomon decoding.

If the number of genuine points among the identified correspondences (*correct matches*) is at least k , the secret polynomial can be recovered. However, if the set of correspondences also comprises chaff points (*false matches*), the number of correct matches must be greater than k , or the decoding must operate on subsets of the matches resulting in many trials. Details are given in Section II-G.

In the original fuzzy vault scheme, correspondence between points in the query set and the fuzzy vault means equality (of the encodings in the finite field). However, for the application of the fuzzy vault to fingerprints the definition of this correspondence is usually adjusted to allow a compensation of noise in the measurement of the minutiae. Following the approach of [7] and [6], we define correspondence as mappings determined by a minutiae matching algorithm (see Section II-D).

The fuzzy vault scheme is error tolerant with respect to the set difference metric, which covers exactly the errors introduced to (naively encoded) minutiae information by insertions, omissions, and permutation of minutiae. The deployment of a minutiae matching algorithm for identifying correspondences between the query set and the fuzzy vault adds robustness with respect to global rotations and translations or non-linear deformations of the fingerprint. Since the matching algorithms included in standard fingerprint software only outputs a match score

and not the list of corresponding minutiae, we use our own matching algorithm (see Section II-D).

In some cases even a random set of points from the fuzzy vault will result in the recovery of a polynomial, but with high probability it will not be the polynomial P derived from the secret. In order to allow verification of the correctness of the recovered polynomial, we amend the scheme by storing a hash value of the polynomial's coefficients. If a secure cryptographic hash function is used, we can assume that the hash value can not be used to recover the secret polynomial.

C. Multi-biometric fusion

In order to obtain sufficient information for a secure scheme, we use multiple instances of fingerprints. Specifically, we use the imprints of $f \geq 2$ fingers of each person. The information extracted from the individual instances (the fingers used) can be merged at various levels [12]: at sensor level, feature level, score level, and decision level. Sensor level fusion introduces additional complexity when single finger sensors are used, because they need to be merged after acquisition. On the other hand, score level fusion and decision level fusion are generally not eligible for multi-instance biometric template protection, because it implies the usage of individual secrets (polynomials in the case of the fuzzy vault) for each feature or instance; this enables separate brute force attacks on each biometric instance (in our case on each finger) individually, resulting only in a linear increase of security with the number of instances (fingers) used. In contrast, in case of feature level fusion a single secret key is bound to the merged information of all instances, and a brute force attack needs to determine the biometric information of all instances simultaneously, resulting in an exponential increase of security with the number of instances.

For these reasons, we implemented feature level fusion by encoding the minutiae of all fingers in one feature vector. In this vector each minutiae is encoded as a triplet (θ, a, b) , where $\theta \in \{1, \dots, f\}$ is an index of the finger on which the minutiae was detected, while a and b denote the Cartesian coordinates of the minutiae location in the fingerprint image of the respective finger. Chaff points are encoded analogously.

D. Minutiae matching algorithm

We need to identify matching minutiae between fingerprints for enrollment and for verification: during enrollment minutiae matching is used to identify the most reliable minutiae from several measurements. During verification we have to identify a sufficiently large set of genuine minutiae within the vault to recover the secret polynomial.

The matching is performed for each finger separately by a simple matching algorithm that identifies minutiae correspondences between two sets M and \bar{M} of points \mathbf{m}

(minutiae or chaff points) which are given by their positions (a, b) in the fingerprint image. The algorithm tries to maximize the number of correspondent points between the sets by finding a suitable global rotation and translation transformation T and tolerates (Euclidean) distances $\|\cdot\|_2$ between two points smaller than δ , where δ is a parameter of the algorithm. Further parameters are a tolerance ϵ for the comparison of distances between minutiae and the limits for rotation ω and translation S , which are introduced to limit the computational complexity of the algorithm.

Algorithm 1 Minutiae Matching Algorithm

Input: Sets $M = \{\mathbf{m}_1, \dots, \mathbf{m}_n\}$ and $\bar{M} = \{\bar{\mathbf{m}}_1, \dots, \bar{\mathbf{m}}_{n'}\}$ of (minutiae or chaff) points with $\mathbf{m}_i, \bar{\mathbf{m}}_i \in \mathcal{E}$.

for all $1 \leq i < j \leq n$ **do**
 Set $D_{ij} = \|\mathbf{m}_i - \mathbf{m}_j\|_2$.
end for

for all $1 \leq i' < j' \leq n'$ **do**
 Set $D'_{i'j'} = \|\bar{\mathbf{m}}_{i'} - \bar{\mathbf{m}}_{j'}\|_2$.
end for

for all $1 \leq i < j \leq n$ **do**
 for all i', j' with $|D_{ij} - D'_{i'j'}| \leq \epsilon$ **do**
 Identify the isometry $T = (\phi, \mathbf{v})$ so that $T(\mathbf{m}_i) = \bar{\mathbf{m}}_{i'}$ and $T(\mathbf{m}_j) = \bar{\mathbf{m}}_{j'}$.
 if rotation and translation are within the configured limits, i.e., $|\phi| < \omega$ and $\|\mathbf{v}\|_2 < S$ **then**
 Apply isometry T to all points in B .
 Identify set C_T of pairs $(\mathbf{m}_\alpha, T(\bar{\mathbf{m}}_\beta))$ so that \mathbf{m}_α and $T(\bar{\mathbf{m}}_\beta)$ have distance smaller than δ and are the closest matches for each other.
 end if
 end for
end for

return Isometry T and set of minutiae mappings C_T for which $|C_T|$ is maximal.

A pseudo code description is given in Algorithm 1. Since we apply the minutiae matching algorithm for each finger separately, no finger index is used.

Our experiments revealed that $\epsilon = 0.2$, $\omega = 45^\circ$, and $S = 200$ (pixels) already yield relatively good matching results (after pre-alignment of the images as described in Section II-E6), while larger values increase the running time considerably without significant improvement of the matching rate. Therefore, we fixed these parameters to these values.

The tolerance parameter δ varies: we use a greater value $\delta = \delta_e$ for enrollment than the value $\delta = \delta_v$ for verification to increase the number of reliable minutiae.

E. Optimizations

1) *Restriction of fingerprint area:* Since fingerprints usually assume an oval shape, minutiae rarely occur in

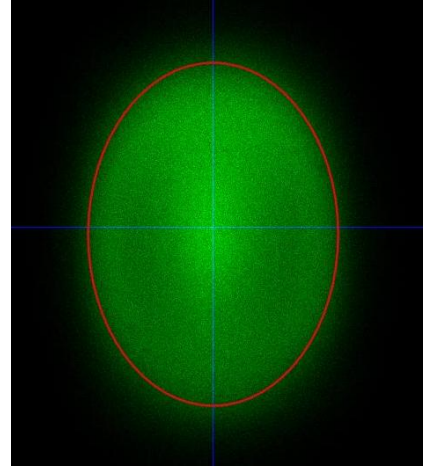


Fig. 1. Distribution of minutiae positions in 82800 fingerprints and the ellipse \mathcal{E} from where minutiae are considered. The brightness of pixels corresponds to the frequency of minutiae occurrence at this position.

the corners of the image, provided that the sensor area is sufficiently large. In order to ensure that the distribution of the randomly selected chaff points resembles that of genuine minutiae, we restrict both the chaff points and the minutiae considered in the vault to an area \mathcal{M} with sufficiently high minutiae occurrence. Such an area was empirically determined by a statistical evaluation of the positions of 5.8 million minutiae extracted from 82800 imprints taken from 9200 fingers with 3 different sensors having 500 DPI.¹ It turned out that - independent of the finger - 7/8 of all minutiae occurred in an area defined by an ellipse \mathcal{E} that covers approximately 87000 pixels, which roughly corresponds to 2.25 cm². The distribution of the minutiae positions and the ellipse are shown in Figure 1. Consequently, we choose minutiae and chaff points only from the set \mathcal{M} given by the union of these ellipses on the considered fingers, i.e. $\mathcal{M} := \{(\theta, a, b) \mid \theta \leq f \wedge (a, b) \in \mathcal{E}\}$.

2) *Reliability filtering during enrollment:* In order to minimize minutiae insertion and omission errors, we use only the most reliable minutiae for the feature vector. Several minutiae quality assessment indices have been developed (e.g. [13] or [14]) which could be used to (à priori) predict the reliability of detection of the individual minutiae. However, we anticipate that an empirical (à posteriori) determination of the detection reliability with a sufficient number of samples yields better results. For this reason, we use multiple measurements during enrollment and consider only those minutiae in the feature vector that have been detected in all measurements. Details are given in Section II-F.

3) *Enforcing minimum distance:* Due to the deviations in the measured minutiae locations, it can happen during authentication that a minutia in a query fingerprint is

¹The fingerprints had been collected in a previous project of the BSI and secunet.

closer to a chaff point than to the corresponding minutiae in the vault. Although we try to minimize these deviations by setting the locations of the stored minutiae to their mean value measured during enrollment, the frequency of such assignment errors can drastically increase if the chaff points are selected too close to genuine minutiae. Therefore, we select the chaff points with a minimum distance d to the genuine minutiae of the same finger with respect to the Euclidean distance. Furthermore, in order to prevent that an adversary can exploit this minimum distance to distinguish chaff points from genuine minutiae, we also enforce the minimum distance among the minutiae and chaff points. In particular, if the Euclidean distance between two minutiae on the same finger is smaller than d , one of them is randomly disregarded, and chaff points are selected with minimum Euclidean distance d to all other chaff points and minutiae from the same finger.

4) *Quality filtering during authentication:* In [10], it is shown that the achievable entropy loss of the scheme decreases with an increase of the average number of surplus minutiae (i.e., minutiae not matching with real minutiae in the reference template) per query fingerprint. The reason for this fact is that, on average, the number of *false matches* of minutiae with chaff points increases with the average number of surplus minutiae per query fingerprint. However, an increase of false matches requires stronger error correction by lowering the degree k of the secret polynomial, which decreases security of the scheme with respect to both information theoretic lower bounds and practical attacks.

In order to limit the average number s of surplus minutiae per query fingerprint, we filter the minutiae from the query fingerprint using the quality index value output by the minutiae extraction algorithm. Precisely, we define a minimum quality value Q and provide to the matching algorithm only those minutiae of the query fingerprint that have a quality value of at least Q . In our concrete implementation we used the MINDTCT algorithm of NIST [13] for minutiae extraction which outputs minutiae quality values in the range between 0 and 1.

The motivation for the quality filtering during authentication is that during enrollment only the most reliable minutiae have been used for computing the reference template. Since the quality values of the minutiae should predict their detection reliability, minutiae with higher quality value are more likely to be used for template generation. In practice, however, the quality value of a minutiae considerably varies between different measurements. Furthermore, experiments show that reliable minutiae sometimes have small quality values. This implies that quality filtering would not only reduce the number of false matches but also the number of correct matches. Therefore, the extent of filtering, i.e., the value chosen for parameter Q , must be carefully selected based on empirical data so that the number of correct matches is not significantly reduced.

5) *Enforcement of minimum number of minutiae per finger:* One of the main sources for failures during authentication is the difficulty to correctly align the query fingerprints with respect to the stored minutiae. This task is performed by the minutiae matching algorithm (described in Section II-D) for each finger by identifying the isometry (rotation and translation) that maximizes the number of matches between the minutiae extracted from the query fingerprint and the points (representing minutiae or chaff point) stored in the reference data. However, this approach can only be successful if the reference template contains a sufficient number of minutiae of each finger; otherwise, i.e., if for one of the fingers the reference template contains only few minutiae, the number of wrong matches (with chaff points) resulting by chance from an incorrect isometry may be higher than the number of matches for the correct isometry. In practice, such cases can easily occur if one of the fingerprints captured during enrollment is of relatively poor quality.

For this reason, we require that the reference template computed during authentication contains at least χ minutiae from each finger, where χ is an additional parameter. Since this constraint reduces the number of possible reference templates its impact on security must be analyzed. We provide an estimation of this reduction in Section III-C.

6) *Pre-alignment of fingers and threshold for rotation:* Multi-biometric systems are more laborious and time-consuming for the user than single-biometric systems. This is particularly true for the fuzzy fingerprint vault: for security reasons (see Section II-C for a discussion), the success of the authentication is not evaluated for each finger individually but only for all of them together; this implies that in case of a failure the user does not know which of the fingerprints caused the authentication to fail and, hence, he is forced to re-capture all fingers. However, the following discussion shows that poor quality fingerprints can be quite reliably detected even before the polynomial reconstruction is started.

Our matching algorithm does not rely on a correct alignment of the query fingerprint in relation to the minutiae set contained in the reference template, but it identifies an isometry (rotation and translation) between the set of minutiae of the query fingerprint and the points of the reference template so that the number of matches is maximized. In most cases this approach works well and the matching algorithm outputs many more correct matches than false matches (with chaff points) which indicates that the isometry identified represents the correct alignment of the fingerprints quite exactly. However, in some few cases the number of wrong matches is greater than the number of correct matches, which typically results in a failure to recover the secret polynomial. Our analysis of more than 160 tests performed shows that in most of these cases the rotation applied by the matching algorithm was extraordinarily large, indicating that the identified

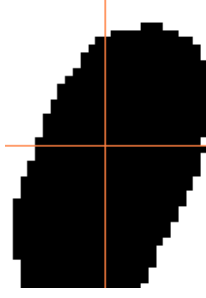


Fig. 2. Uneven distribution of the pixels between the pairs of opposed quadrants triggering a rotation counterclockwise.

isometry was incorrect.

This observation shows that a threshold for the rotation identified by the matching algorithm could be used to detect poor quality fingerprints that result in failed verifications. However, in order to maximize the efficiency of this approach, we should try to minimize the magnitude of the rotation in the correct isometry, i.e., the isometry that correctly maps the minutiae of the query fingerprint to the minutiae in the reference template. We do so by pre-aligning the fingerprints before the minutiae are extracted. Several approaches have been proposed for this task, in particular the detection of singular points (e.g., [15]) or the additional storage of supplementing alignment data (e.g., [16], [17]). However, alignment data may reveal information about the minutiae and singular point detection is quite complex. Therefore, we decided to follow a different approach which is simple and does not require the storage of additional reference data.

Our pre-alignment algorithm scales down the fingerprint image and uses a threshold on pixel brightness to obtain an image displaying the shape of the fingerprint as black area. Furthermore, the image is shifted so that the centroid of all black pixels matches the image center. Then it iteratively performs the following step:

If the sum of black pixels in the upper left and the lower right quadrant exceeds the number of black pixels in the lower left and the upper right quadrant, the image is rotated clockwise by 1° ; else, it is rotated counterclockwise by 1° . Following each rotation the wedge at the lower end resulting from the rotation is removed by horizontal cropping. The evaluation criteria for the rotation is illustrated in Figure 2.

The iteration stops as soon as the direction of rotation changes. Finally, the aggregated rotations are applied to the original fingerprint image.

F. Enrollment

Let $f \geq 2$ be the number of fingers used per person, q a prime power, $k < t < r \leq q$, and $\chi \leq t/f$. For each user, a random polynomial P of degree less than k over the finite field \mathbf{F}_q is selected. The coefficients of this polynomial represent the secret of the scheme. Then, for each finger u imprints are taken and the minutiae correspondences

between these instances are identified using the matching algorithm (Algorithm 1) with tolerance parameter $\delta = \delta_e$. Minutiae outside the considered set \mathcal{M} , i.e., with position outside the ellipse \mathcal{E} on the respective finger, are neglected (see Section II-E1). Then, t of those minutiae that have been detected in all u imprints of the respective finger are selected at random so that at least χ minutiae are taken from each finger and each pair of chosen minutiae has a minimum distance of d . This set T of t reliable minutiae can be considered the biometric template to be protected by the fuzzy vault scheme. The template T is amended with random chaff points, resulting in a set R of r points containing t genuine minutiae and $r - t$ chaff points, so that each point in R has a minimum distance of d to all other points from the same finger. Furthermore, in order to ensure that minutiae and chaff points within the vault are not distinguishable by their order, they are lexicographically ordered.

In contrast to the original fuzzy vault scheme [3], the secret polynomial is redundantly encoded not by evaluating it on the biometric data itself but only on the minutiae's indexes in the ordered list. Precisely, for all $1 \leq i \leq r$ we (re-)define $x_i = E(i)$, where E is an injective embedding from the set $\{1, \dots, r\} \subset \mathbf{Z}$ to \mathbf{F}_q . (For instance, if q is prime we could set $E(i) := i \bmod q$.) Further, we set $y_i = P(x_j)$, if \mathbf{m}_i is a genuine minutia, and choose a random value $y_i \neq P(x_j)$, if \mathbf{m}_i is a chaff point, where j is the index of \mathbf{m}_i after applying the lexicographic order. This optimization allows a reduction of the field size to the range of r . The vault Y is given by the ordered list of minutiae and chaff points, paired with the corresponding y_j values. The vault and a hash value H of the polynomial's coefficients are stored in the database.

A pseudo code description of the enrollment is given in Algorithm 2. There h denotes a collision resistant hash function. Furthermore, both minutiae and chaff points are denoted as $\mathbf{m} = (\theta, a, b)$, where θ is an index of the finger and (a, b) are the Cartesian coordinates of its location in the image. We define the *distance* $\|\mathbf{m} - \mathbf{m}'\|$ of two minutiae on the same finger as the Euclidean distance of their location.

G. Recovery of the polynomial

The unlocking of the vault (during authentication) requires the recovery of the secret polynomial P from a set of points (x_{j_i}, y_{j_i}) , some of which (those resulting from *correct matches* with minutiae) lie on the polynomial, while others (resulting from *false matches* with chaff points) do not. For this task, a Reed-Solomon decoder RSDE-CODE is used that receives as input a set of w points $(x_{j_1}, y_{j_1}), \dots, (x_{j_w}, y_{j_w}) \in \mathbf{F}_q^2$ with $w \geq k$ and outputs $e_0, \dots, e_{k-1} \in \{0, \dots, q-1\}$, so that $y_{j_i} = P(x_{j_i})$ holds for at least k of the (x_{j_i}, y_{j_i}) with $P(z) = \sum_{i=0}^{k-1} e_i z^i$, if such a polynomial exists. We assume that the Peterson-Berlekamp-Massey-decoder is used as suggested in [3]. This technique is successful, if at least $(w + k)/2$ of the w

Algorithm 2 Enrollment

Select a random polynomial $P(z) = \sum_{i=0}^{k-1} e_i z^i$ over \mathbf{F}_q .

for $\theta = 1$ to f **do**

Take u imprints of finger θ and pre-align them (see Section II-E6)

Extract the corresponding sets $M_{\theta,1}, \dots, M_{\theta,u}$ of minutiae.

for $j = 2$ to u **do**

Find correspondences between $M_{\theta,1}$ and $M_{\theta,j}$ using Algorithm 1 with $\delta = \delta_e$.

end for

Identify the set A_θ of *reliable minutiae* that are present in all u imprints.

for all Minutiae $\mathbf{m} \in A_\theta$ **do**

Set $\mathbf{m} = (\theta, a, b)$, where (a, b) is the mean value of its location over the u measurements.

end for

Remove all (θ, a, b) from A_θ with $(a, b) \notin \mathcal{E}$.

while two minutiae have distance smaller than d **do**

Randomly remove one of them.

end while

if $|A_\theta| < \chi$ **then**

Repeat capture process for finger θ .

end if

end for

Set $A = \bigcup_\theta A_\theta$ as the set of all reliable minutiae.

if $|A| < t$ **then**

return “ERROR: Not enough reliable minutiae”

end if

Randomly select $T = \{\mathbf{m}_1, \dots, \mathbf{m}_t\} \subseteq A$ so that T contains at least χ minutiae for each finger.

Randomly select $r - t$ chaff points $\mathbf{m}_{t+1}, \dots, \mathbf{m}_r$ so that $\|\mathbf{m}_i - \mathbf{m}_j\| \geq d$ for all $1 \leq i < j \leq r$.

Compute the lexicographic order $(\mathbf{m}_{j_1}, \dots, \mathbf{m}_{j_r})$ of $R = \{\mathbf{m}_1, \dots, \mathbf{m}_r\}$.

for $i = 1$ to r **do**

if \mathbf{m}_{j_i} is a genuine minutia, i.e., $j_i \leq t$ **then**

Set $y_i = P(x_i)$ with $x_i = E(i)$.

else

Select a random $y_i \neq P(x_i) \in \mathbf{F}_q$.

end if

end for

Set $Y = (\mathbf{m}_{j_1}, y_1, \dots, \mathbf{m}_{j_r}, y_r)$.

Compute $H := h(e_0 || \dots || e_{k-1})$, where $||$ denotes concatenation.

Store Y and H in database.

points handed over to the decoder are correct. Although there are Reed-Solomon-Decoders that can decode with only \sqrt{wk} correct points, they do not offer any advantage for the fuzzy vault, because for typical parameters \sqrt{wk} is quite close to $(w + k)/2$, and they are computationally much less efficient (see [3]).

As pointed out in [4], the Reed Solomon Decoding degenerates to a brute-force polynomial interpolation for $w = k$. Previous implementations of the fuzzy fingerprint vault [4], [5], [6] have used this brute-force approach for decoding. However, numerical evaluation reported in [10] revealed that setting $w = 2m_c - k$ and $k \approx m_c - m_f$ can provide a good balance between efficient decoding and security, where m_c and m_f are the expected numbers of correct and false matches, respectively. However, if the match rate disperses considerably, it may be necessary to slightly deviate from this value, in order to reduce the False Rejection Rate. As we will see in Section IV-B, this is the case.

H. Authentication

We only implement an authentication in the verification scenario, where the identity of the (alleged) user is known a priori.

In order to verify the identity of a user, a query fingerprint is taken for each considered finger. The minutiae are extracted and matched with the minutiae and chaff points \mathbf{m} contained in the vault stored for the alleged user. The indices of those minutiae and chaff points in the vault matching with minutiae in the query fingerprint are identified; along with the corresponding y_i values they are given to RSDECODE (see Section II-G) to recover the secret polynomial P . If the number of genuine minutiae among these points is sufficiently high (see Section II-G for a discussion), the polynomial can be recovered. Finally, the correctness of the recovered polynomial is verified using the hash value stored in the database. Optionally, the secret key (given by the coefficients of the recovered polynomial) can be used for further cryptographic applications, e.g., as seed in a key derivation function.

A pseudo code description of the verification is given as Algorithm 3. The tolerance parameter δ_v used for the minutiae matching algorithm can differ from that used during enrollment.

III. SECURITY ANALYSIS

In this contribution we consider the security of the fuzzy vault for multiple fingerprints with respect to attacks that try to recover the minutiae or, equivalently, the secret polynomial from the vault. It is understood that there are other types of attacks against biometric template protection schemes to which the fuzzy vault is susceptible [18]. In particular, the cross matching of the vaults from several independent enrollments of a user represents a serious threat to the fuzzy vault. However, a comprehensive analysis of all potential attacks against the fuzzy vault would go beyond the scope of this paper.

A. Provable Security

In [10], lower bounds on the security of the fuzzy fingerprint vault were deducted. In particular, for the case $r = q$ and $\chi = 0$, an upper bound was given for

Algorithm 3 Verification of a user's identity

Select Y and H stored in database for this user
Set $I = \emptyset$.
for $\theta = 1$ to f **do**
 Identify in Y the subset R_θ of minutiae and chaff points on finger θ .
 Take a query fingerprint for finger θ and pre-align it as described in Section II-E6.
 Extract the set M_θ of minutiae with quality value at least Q (see Section II-E4).
 Find correspondences between R_θ and M_θ using Algorithm 1 with $\delta = \delta_v$.
 for all $\mathbf{m} \in R_\theta$, which have matched a minutia in M_θ **do**
 Add (x_i, y_i) to I , where $x_i = E(i)$ and i is the index of \mathbf{m} in Y .
 end for
end for
for all Subsets Z of I with cardinality x **do**
 Start RSDECODE on input Z (see Section II-G).
 if RSDECODE outputs $\bar{e}_0, \dots, \bar{e}_{k-1}$. **then**
 if $\bar{H} = h(\bar{e}_0 || \dots || \bar{e}_{k-1}) = H$ **then**
 return "Verification successful".
 Optional: Return $\bar{e}_0 || \dots || \bar{e}_{k-1}$.
 Stop algorithm.
 end if
 end if
end for
return "Verification not successful"

the success probability of any algorithm that takes as input the vault Y and tries to output the corresponding secret polynomial or the corresponding template T . The analysis conducted in [10] revealed that a security of at least 50 bits can only be achieved if the match rate, i.e., the rate of minutiae in the vault matched with the query fingerprints during verification, exceeds a certain minimum value which depends on the average number s of surplus minutiae (i.e. the minutiae that do not match with a genuine minutia in the template) per query fingerprint and on the tolerance parameter δ_v used for matching during verification.

B. Existing attacks

The most efficient method to recover the minutiae or secret polynomial from the vault was published by Mihailescu [8]. This brute force attack is designed to break the implementations of [4], [5] and [6]; in the context of our scheme it is even slightly more efficient as the correctness of the recovered polynomial can be verified using the hash value of the secret coefficients and does not require additional evaluations of the polynomial. With this adaptation the attack systematically searches through all subsets $\{i_1, \dots, i_k\}$ of $\{1, \dots, r\}$, computes the unique polynomial P satisfying $P(E(i_j)) = y_{i_j}$ by Lagrange interpolation,

and checks the correctness of this polynomial with the stored hash value. According to [8], the number of trials needed is $1.1(r/t)^k$ and each trial requires $6.5k \log^2(k)$ arithmetic operations over \mathbf{F}_q .² However, in the latter estimation an explicit constant of 18 for multiplication of the polynomials (see Corollary 8.19 in [19]) has been overlooked, and thus, we end up with a total number of approximately $129k \log^2(k)(r/t)^k$ arithmetic operations.

If the number of chaff points is close to the maximum possible, the attack described in [20] can be more efficient than brute force. The basic idea is that the free area around chaff points is smaller than around genuine minutia. Assuming a density 0.45 for random sphere packings [4], the maximum number of chaff points per finger would be $0.45 \cdot 87000/V_d$, where V_d is the number of integer point in the sphere of radius d .

Another threat to the fuzzy fingerprint vault is the *fingerprint dictionary attack*, where an attacker simulates verification with the vault using a large number of real or artificial fingerprints. If the templates are chosen according to a realistic distribution, the success probability of each attempt equals the False Accept Rate (FAR) and the attacker needs $(\text{FAR})^{-1}$ trials on average. Therefore, if a single simulation of verification takes C computational steps, the attack's running time is $C \cdot (\text{FAR})^{-1}$. Note, that simulation involves templates extraction and minutiae matching, which are computationally much more expensive than a polynomial interpolation.

Unfortunately, determination of very small FAR values is computationally very expensive: While the FAR for the multi-finger setting (i.e. for $f \geq 2$) can be extrapolated from the FAR of a single-finger setting, determination of latter one requires considerably more than FAR^{-1} matching operations and must be performed for each set of parameters individually. For the security level we aim at, this already takes more time than we have available for this publication. Therefore, we do not evaluate the security with respect to the fingerprint dictionary attack, but leave this task to a future publication.

C. Entropy loss by the minimum number of minutiae per finger

Whereas the enforcement of a minimum number χ of minutiae per finger (see Section II-E5) aims at reducing the false rejection rate it also decreases the security of the scheme by narrowing the set of possible templates. This applies to the lower bound on attacks according to [10] as well as to the practical attack of [8]. The subsequent analysis quantifies this reduction of security.

We will assume that the minutiae chosen are independently and uniformly distributed among the F fingers. This assumption can be fulfilled by a suitable probabilistic

²In fact, the number of trials needed is considerably higher, as the estimate $\binom{r}{k}/\binom{t}{k} < 1.1(r/t)^k$ used in [8] for $r > t > 5$ does not hold true.

selection method of the template T from the set of reliable minutiae during enrollment.

Using this assumption and the inclusion-exclusion-principle, we can estimate the probability $\zeta(t, \chi)$ that a template with t minutiae includes for each finger f at least χ minutiae by

$$\zeta(t, \chi) = 1 - f^{-t} \sum_{\theta=1}^f (-1)^{\theta} \binom{f}{\theta} \cdot \sum_{i_1, \dots, i_{\theta}=0}^{\chi} \binom{t}{i_1, \dots, i_{\theta}, t - \sum_j i_j} (f - \theta)^{t - \sum_j i_j},$$

where $\binom{a}{b_1, \dots, b_m}$ with $b_1 + \dots + b_m = a$ denotes the multinomial coefficient.

On the other hand, the conditional probability p that a particular instance of a template T is chosen, if a minimum number of χ minutiae per finger is enforced, can be calculated from the probability p' that this instance is chosen, if no minimum number of minutiae per finger is enforced, by the equation $p = p' / \zeta(t, \chi)$. Therefore, the entropy $\mathbf{H}_{\infty}(T_{\chi})$ of a template chosen with a minimum number of minutiae per finger is exactly $\log \zeta(t, \chi)$ smaller than the entropy of a template chosen without a minimum number of minutiae per finger.

For practical attacks, the search space is narrowed by the factor $\zeta(t, \chi)$; thus, the best known attack could be adapted to require at most $129\zeta(t, \chi)k \log^2(k)(r/t)^k$ operations.

IV. RESULTS

In this section, we summarize the results of empirical parameter evaluations, the impact of the individual optimizations, and the general performance of the scheme.

We used a test set of 864 fingerprints taken from 18 persons in the course of this research using an optical sensor, each person providing 6 imprints of 8 fingers (little fingers were excluded). In our experiments, we used 6 or all 8 fingers per person (without or with thumbs), but results referring to single fingers were averaged over all finger types.

For minutiae extraction, we used the MINDTCT algorithm of NIST [13]. We stress that other feature extraction algorithms may exhibit a different performance, and therefore, the resulting statistics may deviate from ours.

A. Size of feature vector

First, we determined how large the feature vector can be in dependence of the number u of measurements and the tolerance parameter δ_e used during enrollment. We did this by evaluating the number of minutiae per finger that are reliably (i.e., u times) detected in u measurements. Since this number varies considerably among individuals and measurements, acceptable Failure To Enroll (FTE) rates can only be achieved, if the required number of reliable minutiae is considerably lower than its average value. Therefore, we evaluated the maximum number M_r

TABLE I
NUMBER M_r OF RELIABLE MINUTIAE PER FINGER THAT IS FOUND IN 80% OF ALL MEASUREMENTS.

u	$\delta_e = 5$	$\delta_e = 7$	$\delta_e = 10$	$\delta_e = 15$
1	63	63	63	63
2	23	32	39	43
3	18	24	31	35
4	9	16	22	27
5	6	9	15	18

of reliable minutiae that is achieved in at least 80% of all measurements. The results of this evaluation are listed in Table I.

In the multi-biometric setting, a single finger having only few reliable minutiae can be compensated by the others. However, in the case of only two fingers, this effect is smaller than for $f \geq 3$. Moreover, if an individual generally has low quality fingerprints, e.g. due to skin abrasion, cuts or dry skin, the probabilities that several fingers have few reliable minutiae are dependent and do not multiply. Therefore, the required number of reliable minutiae should be carefully selected based on empirical evaluation of the resulting enrollment error rates.

Due to the small number of reliable minutiae for $u = 5$, we generally recommend to set $u \leq 4$.

B. Minutiae matching rates

In order to configure the error correction capabilities of our scheme appropriately, it is necessary to determine the rate at which the genuine minutiae in the vault are identified during authentication. For various tolerance parameters $\delta_v = \delta_e$, we computed the biometric template set T , containing t minutiae reliably detected in u measurements, and matched them with the minutiae of an (independent) query fingerprint using our matching algorithm. We did not add chaff points to the template T . The average match rate, i.e. the average ratio between the number of matches found and t , are given in Table II.

Similarly to the number of reliable minutiae, the match rate varies considerably between different measurements. Moreover, in the presence of chaff points, the match rates slightly decrease depending on the expected number of false matches (with chaff points), as the chaff points render the correct mapping of the minutiae more difficult for the matching algorithm. (This aspect is further discussed in Section IV-F.) Therefore, a reasonably small FRR can only be achieved if k is selected slightly smaller than the

TABLE II
AVERAGE MATCH RATE (IN PERCENTAGE) IN THE ABSENCE OF CHAFF POINTS FOR $\delta_e = \delta_v$.

u	$\delta_v = 5$	$\delta_v = 7$	$\delta_v = 10$	$\delta_v = 15$
1	40	50	58	64
2	66	72	78	82
3	75	81	84	87
4	81	85	88	90
5	85	89	91	92

TABLE III
EXPECTED NUMBER OF MINUTIAE IN A QUERY FINGERPRINT AFTER
FILTERING WITH MINIMUM QUALITY VALUE Q .

Minimum quality Q	Av. no. τ of minutiae
0	70
0.1	67
0.2	52
0.3	48
0.4	41
0.5	33
0.6	32

expected value of $m_c - m_f$ (see Section II-G). Our empirical evaluation suggests to set k 10%-20% smaller than this value.

For $2 \leq u \leq 4$, we obtain good match rates at a reasonable number of minutiae. Therefore, we will subsequently focus on these cases.

C. Effect of quality filtering during verification

As argued in Section II-E4, quality filtering of the minutiae in the query fingerprints aims to reduce the number of surplus minutiae, i.e., minutiae in the query fingerprints that do not match with genuine minutiae in T . We evaluated the effectiveness and eligible configuration of the filtering based on the minutiae quality values output by the MINDTCT algorithm of NIST [13].

A statistic evaluation on our test set revealed that the distribution of the minutiae quality values output by the MINDTCT is very uneven; values in certain ranges occur very frequently while others (e.g., between 0.5 and 0.57) are almost never assumed.

The average number of minutiae detected in a single fingerprint depends on the sensor used, the feature extractor algorithms, the quality of the images, and even the finger type (e.g. thumbs contain more minutiae than other fingers). In our tests, we detected an average number of 84 minutiae per fingerprint (excluding thumbs) inside ellipse \mathcal{E} . Based on this number and the distribution of quality values, we can estimate the expected number τ of minutiae in a query fingerprint after filtering with minimum quality value Q . The results are listed in Table III.

The reduced average number τ of minutiae per query finger given to the matching algorithm results in a decreased average number s of surplus minutiae per finger and in less false matches (i.e., matches with chaff points). On the other hand, it may also reduce the number of correct matches (and likewise the match rate) because the minutiae filtered out could have matched with genuine minutiae in the vault. For different sets of parameters we empirically determined the decrease of the number of correct and false matches resulting from the quality filtering. An example plot is presented in Figure 3.

For larger r and smaller δ_v , quality filtering with higher values of Q results in a more drastic reduction of the correct matches. Nevertheless, for various parameters we consistently found a value Q between 0.2 and 0.3 to be

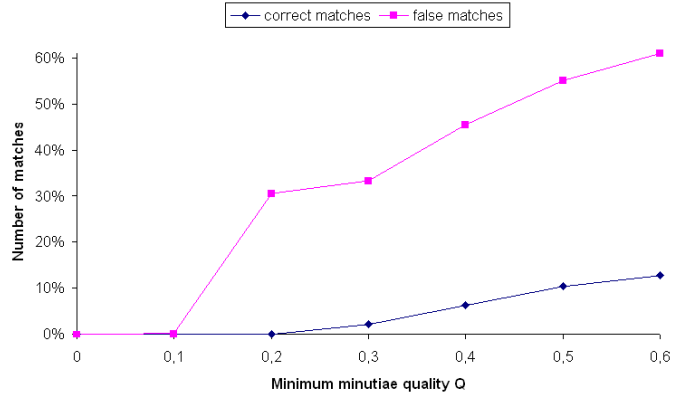


Fig. 3. Reduction of the correct and false matches by quality filtering for $f = 6$, $t = 120$, $r = 400$ and $\delta_v = 7$.

optimal, reducing the false matches by approximately 30% while decreasing the number of correct matches by less than 3%.

D. Effect of minimum number of minutiae per finger

If the tolerance parameter δ_v is set appropriately as described in Section IV-F, the number of correct matches typically exceeds the number of false matches. On the other hand, if the matching algorithm fails to identify the correct isometry, the number of correct matches is typically significantly lower than the number of false matches. As explained in Section II-E5, the enforcement of a minimum number χ of minutiae per finger in the template T aims at reducing the frequency of such cases. We evaluated the effectiveness and reasonable configuration of this optimization by determining the ratio of fingers for which the number of false matches exceeded the number of correct matches for various values of the parameter χ . Furthermore, we analyzed the influence of this optimization to the FTE by determining the rate at which a finger contained at least χ minutiae and, hence, would succeeded to enroll. The results of this evaluation are displayed in Figure 4 by the curves of the match rate and the rate of successful enrollment. (Other failures of enrollment, particularly cases, where the fingers of a person contained less than t minutiae in total, were neglected.) Obviously, $\chi = 9$ already yields a considerable improvement with only moderately increased FTE rates.

The impact of the value of χ becomes particularly strong as the average number of false matches approaches the number of correct matches. As shown in Figure 5 for $f = 6$, $u = 4$, $t = 100$, $r = 600$, $\delta_e = 10$, $\delta_v = 7$ and $Q = 0.3$, where even for $\chi = 15$ the fraction between the average numbers of correct and false matches was 2.1 (as opposed to a fraction of 2.9 for the parameters of Figure 4), the average match rate steadily and considerably increases until $\chi = 15$. The decrease of the successful enrollment rate is similar to the case of Figure 4. This finding indicates that in these cases it may be worth to choose χ larger than

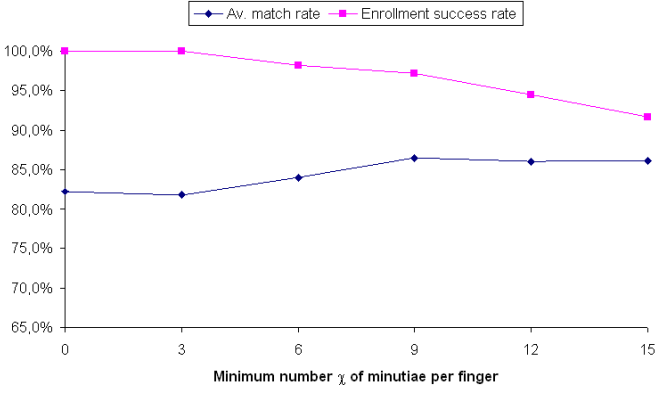


Fig. 4. Impact of enforcing a minimum number χ of minutiae per finger in T to match rate and rate of successful enrollment for $f = 6$, $u = 4$, $t = 120$, $r = 400$, $\delta_e = 10$, $\delta_v = 7$ and $Q = 0$.

9 at the cost of higher FTE rates.

E. Effect of pre-alignment of fingerprints

We evaluated the impact of the pre-alignment of the fingerprints on our test set. We used two sets of parameters with 6 fingers ($f = 6$), the first one being $f = 6$, $u = 4$, $t = 120$, $r = 400$, $\chi = 15$ and $\delta_v = 7$ and the second one being $f = 6$, $u = 4$, $t = 100$, $r = 455$, $\chi = 13$ and $\delta_v = 5$.

On average, the pre-alignment reduced the absolute rotation identified by the minutiae matching algorithm from 4.3° to 2.7° . Much more important than that is the increasing correlation of a failure of the matching algorithm to correctly map the minutiae sets (resulting in more false than correct matches) to the size of the rotation angle. This allows setting up a threshold for the absolute rotation to reliably detect and reject individual query fingerprints for which the minutiae matching algorithm could not determine the correct mapping. In empirical tests, we evaluated the impact of the pre-alignment to the reliability at which a rotation threshold can sort out “bad” fingerprints that contribute more false than correct

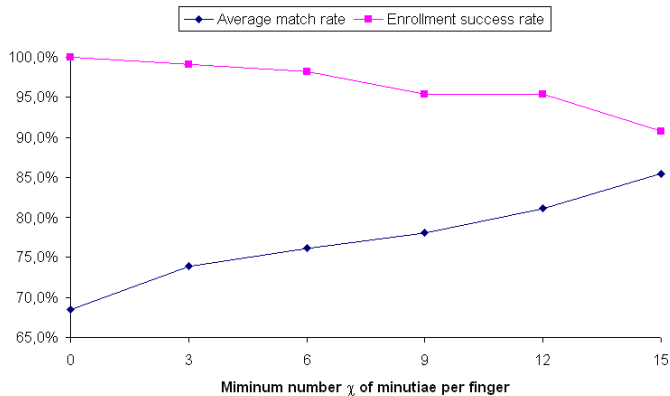


Fig. 5. Impact of enforcing a minimum number χ of minutiae per finger in T to match rate and rate of successful enrollment for $f = 6$, $u = 4$, $t = 100$, $r = 600$, $\delta_e = 10$, $\delta_v = 7$ and $Q = 0.3$.

matches. Without the pre-alignment, a rotation threshold of 10° rejected 86% of those “bad” fingerprints, at the cost of 35% false positives, i.e. “good” fingerprints being rejected. In contrast, when using the pre-alignment described in Section II-E6, a rotation threshold of 8° rejected 100% of the “bad” fingerprints at the cost of only 20% false positives.

F. Balancing correct and false matches

In order to enable the minutiae matching algorithm to determine the correct isometry by which the query fingerprint is correctly aligned to the minutiae in the vault, we must ensure that, on average, the number of correct matches considerably exceeds the number of false matches. The results of Section IV-D indicate that a fraction of 2 between the average numbers of correct and false matches already requires large values for χ which considerably increases the FTE.

In [10], the expected number m_f of false matches is estimated by $(r - t)sV_{\delta_v}/|\mathcal{E}|$, where $V_\delta = 1 + 4 \sum_{i=1}^{\lfloor \delta-1 \rfloor} \lfloor \sqrt{\delta^2 - i^2} \rfloor$ is the number of integer points in the 2-dimensional plane with Euclidean norm smaller than δ and s is the average number of surplus minutiae (i.e., minutiae not matching with genuine minutiae) per query fingerprint. On the other hand, we can estimate $s \approx \tau - \mu t/f$, where τ is the average number of minutiae per query fingerprint after quality filtering.

Our experiments show that for typical parameters the average number of false matches is 20%-60% larger than these estimations imply, depending on the specific parameters. The deviation is presumably due to those outliers resulting from an incorrect determination of the isometry: if the matching algorithm is unable to detect the correct alignment, its optimization strategy with respect to the number of matches will yield extraordinary many false matches. Based on this observation, we adjust our above estimation to

$$m_f \approx 1.4(r - t)(\tau - \mu t/f)V_{\delta_v}/|\mathcal{E}|. \quad (1)$$

Yet, we expect the number of false matches to grow linearly with V_{δ_v} , which is a quadratic function in δ_v .

On the other hand, the average number m_c of correct matches is given by μt , where μ is the match rate, and therefore, grows slowly with increasing δ_v as shown in Table II. Therefore, the selection of δ_v should carefully balance the expected numbers of correct and false matches. For $f = 3$, $u = 4$, $t = 66$, $r = 320$ and $Q = 0.3$, and for $5 \leq \delta_v \leq 15$ we estimated the number of false matches by (1) and the number of correct matches as μt using the match rates empirically determined. The results show that, for these parameters, $\delta_v \leq 8$ should be selected to ensure that the average number of correct matches is at least twice the number of correct matches.

For a smaller ratio r/t , the curves meet at higher values of δ_v , but still the accelerating growth of the number of false matches implies that $\delta_v \leq 8$ is a good choice.

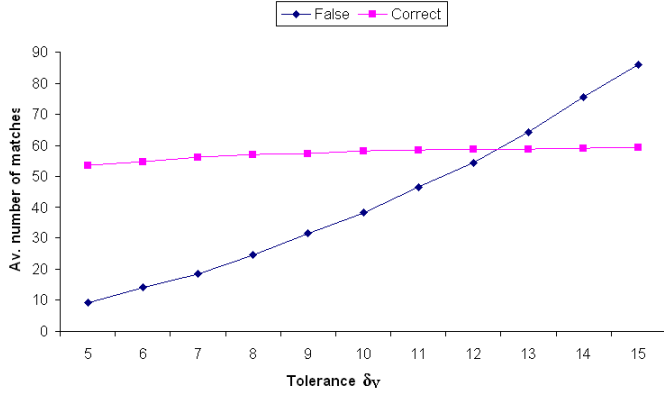


Fig. 6. Impact of the tolerance parameter δ_v on the estimated average number of correct and false matches for $f = 3$, $u = 4$, $t = 66$, $r = 320$ and $Q = 0, 3$.

G. Provable security

In [10], minimum match rates are estimated that are necessary to provide provable security based on the lower bounds given in [11]. These minimum match rates depend on the tolerance parameter δ_v and the number s of surplus minutiae in the query fingerprint (i.e., the minutiae not matching with genuine minutiae of the template) by which the number of false matches is estimated. A comparison of these minimum match rates with the empirically determined rates in Table II (which have been roughly confirmed in the presence of chaff points with appropriate optimizations applied) shows that in practice a provable secure fuzzy fingerprint vault could only be possible for $\delta_v \leq 7$ and $s \leq 20$. As argued in Section IV-F we can estimate $s \approx \tau - \mu t / f$, where τ is the number of minutiae of the query fingerprint after quality filtering. Furthermore, the results of Section IV-C show that quality filtering should not be expected to reduce τ significantly below 48. This implies that $s = 20$ can only be achieved for $\mu t / f \geq 28$. However, evaluation of the values t/f and μ given in Tables I and II, respectively, for $\delta_v \leq 7$ reveals that this condition is only met for $u \leq 2$, where the match rates are much lower than the minimum match rates derived in [10].

Furthermore, as argued in Section IV-F, the false match rates observed in practice are 20% to 60% higher than the estimation in [10] would imply. This means that the value for s must even be decreased to 12-17 to obtain provable security with the minimum match rates given for $s = 20$.

As a summary, we conclude that provable security seems out of reach, unless the average number of surplus minutiae per query fingerprint can be further reduced by improved quality filtering methods.

H. Selection of parameters

For the selection of eligible parameters for a fuzzy fingerprint vault secure against existing attacks, we suggest the following method:

- 1) Define the number of fingers used.
- 2) Set the number of captures per finger for enrollment to $u = 3$ or, preferably, $u = 4$.
- 3) Choose δ_e between 5 and 15, and $t \leq f M_r(\delta_e)$, where $M_r(\delta_e)$ is the number of reliable minutiae for δ_e indicated in Table I. The choice of δ_e and t should be carefully tested with respect to the FTE rate.
- 4) Choose δ_v between 5 and 7. Smaller values may drastically reduce the match rates, which makes it difficult to achieve a high security level. (Note, that setting δ_v much smaller than δ_e may result in smaller match rates than indicated in Table II.) Larger values will result in too many false matches (see Section IV-F).
- 5) Set the minimum distance d between the minutiae and chaff points in the template to approximately $(3/2)\delta_v$ to reduce the probability that a minutiae in the query fingerprint is closer to a chaff point than to its counterpart in T .
- 6) Set Q between 0.2 and 0.3.
- 7) For a broad range of values for r , numerically estimate the expected numbers m_c and m_f of correct and false matches, respectively, by μt and (1) using match rate μ indicated for the selected u and δ_v in Table II and the estimate $\tau \approx 50$. Then, for each value of r set k 10%-25% smaller than $m_c - m_f$ (see Section IV-B) and compute the security against existing attacks as $129\zeta(t, \chi) k \log^2(k) (r/t)^k$. Select the pair r, k for which the security is maximized.
- 8) Select $\chi = 9$, if the fraction between the estimates for the average number of correct and false matches is at least 2.7. Otherwise, increase χ up to 15, depending on this fraction. However, ensure that the fraction is at least 2, if necessary, by decreasing r or δ_v .
- 9) If the maximum security determined is higher than the level aimed at, lower r and k to reduce the false rejection rate (FRR), and decrease t to reduce the failure to enroll (FTE) rate.
- 10) Empirically evaluate the average number of correct and false matches. If these numbers significantly deviate from the estimations used in the previous step, repeat this step with appropriate correction factors.

Based on our statistical data and the method described above, the example parameters listed in Table IV have been determined to provide the indicated security level against existing attacks. We did not experimentally determine real error rates during enrollment and verification; therefore, these parameters are mere suggestions which require practical validation. We set $d = \lfloor 3/2 \cdot \delta_v \rfloor$, $Q = 0.3$ and, as the fraction computed in step 8 above was always greater than 3, $\chi = 9$. Furthermore, we choose $r < \lfloor 0.2 \cdot 87000 / V_d \rfloor$, which is less than half of the maximum value possible, to avoid the attack described in [20] (see Section III-B) that could significantly reduce security.

TABLE IV
PARAMETERS FOR A SECURITY LEVEL OF 2^{Sec} .

f	u	δ_e	δ_v	t	r	k	Sec
2	2	7	5	62	240	27	68
3	2	7	5	90	202	45	69
3	2	7	5	90	351	41	97
3	3	7	5	70	360	34	97

I. Practical evaluation

In order to test the performance of our fuzzy fingerprint vault and its optimizations under realistic circumstances, we enrolled 10 persons using 6 fingers (i.e., $f = 6$) using the parameters $u = 4$, $t = 120$, $r = 400$, $k = 53$, $\delta_e = 10$, $\delta_v = 7$, $\chi = 15$ and $Q = 0.3$. For these parameters, the best known attack requires 2^{100} operations; thus, a security equivalent to 100 bit keys is achieved. For the persons that had been successfully enrolled, we performed a verification. As capture device, we used an optical multi-finger sensor (Cross Match L SCAN Guardian), the NBIS package of NIST (in particular, NFSEG and MINDTCT) [13] for fingerprint segmentation and feature extraction.

First, we evaluated the performance of the enrollment by its FTE and duration. It was aborted after 3 unsuccessful attempts per finger and the FTE was computed as the fraction of aborted enrollments. Furthermore, we determined the average number of retries (repetition of capturing) needed per user (summed up for all fingers) and the time needed.

In order to assess the reliability of the verification, we evaluated the FRR (without any repeated attempts). The FAR for this small sample was zero.

We performed the simulation for two versions of the scheme independently: the first simulation was performed for a basic version without the quality filtering of the minutiae during verification (Section II-E4), the pre-alignment of fingerprints (Section II-E6), and the enforcement of a minimum number of minutiae per finger in the template (Section II-E5). The second version implemented these optimizations. The results of the simulation are listed in Table V.

V. CONCLUSIONS

Our analysis shows that a fuzzy vault for multiple fingerprints can be very secure against template recovery from the helper data, if appropriate optimizations are

³The only failed verification succeeded in the second attempt.

TABLE V
PERFORMANCE OF THE SCHEME IN A SIMULATION WITH 10 PERSONS.
DURATION IS GIVEN IN MINUTES.

	Enrollment			Verification FRR
	FTE	Retries	Duration	
Basic	20%	0.5	2.1	25%
Optimized	0%	2	3.5	10% ³

applied. Filtering minutiae for reliability during enrollment and for quality during verification turn out to be particularly effective. Furthermore, enforcing a minimum number of minutiae per finger in the template significantly increases matching performance. Both optimizations are very sensitive to the respective thresholds, which must be carefully set on the basis of empirical data. Interestingly, we were able to solve the fingerprint alignment problem using a simple algorithm and without storing additional helper data or using singular point detection.

Although we did not achieve match rates required to prove the security by information theoretic arguments as discussed in [10], we can obtain a security level against existing attacks of 2^{70} for two fingers and of 2^{97} for three fingers.

Our simulation of enrollment and verification indicates that the scheme can be effective and efficient in practice. The process of capturing several fingers can be facilitated using multi-finger sensors. Nevertheless, the parameters need to be selected with care to reduce the error rates and effort for enrollment. Furthermore, simulation tests on a larger scale would be needed to obtain more reliable data on achievable error rates. In particular, it would be interesting to investigate the fraction of fingers or persons that consistently fail to provide a sufficient number of reliable minutiae.

Finally, we would like to stress that our security analysis only covered template recovery attacks. Other types of attacks have been published [18] and need to be addressed before the scheme can be considered ready for use. We encourage research on methods to harden the fuzzy fingerprint vault against these attacks.

ACKNOWLEDGMENTS

This work was conducted as part of the projects “BioKeyS-Multi” and “BioKeyS Pilot-DB” of the Bundesamt für Sicherheit in der Informationstechnik.

The matching algorithm was designed and implemented by Stefan Schürmans.

REFERENCES

- [1] J. Merkle, M. Niesing, M. Schwaiger, H. Ihmor, and U. Korte, “Performance the fuzzy vault for multiple fingerprints (short version),” in *BIOSIG 2010: Biometrics and Electronic Signatures*, ser. LNI. Gesellschaft für Informatik, 2010, in press.
- [2] J. Breebaart, C. Busch, J. Grave, and E. Kindt, “A reference architecture for biometric template protection based on pseudo identities,” in *BIOSIG 2008: Biometrics and Electronic Signatures*, ser. LNI, A. Brömme and C. Busch, Eds., vol. 137. Gesellschaft für Informatik, 2008, pp. 25–38.
- [3] A. Juels and M. Sudan, “A fuzzy vault scheme,” in *Proc. IEEE Int. Symp. Inf. Theory*. IEEE, 2002, p. 408.
- [4] C. Clancy, N. Kiyavash, and D. Lin, “Secure smartcardbased fingerprint authentication,” in *WBMA ’03: ACM SIGMM workshop on Biometrics methods and applications*. ACM, 2003, pp. 45–52.
- [5] U. Uludag, S. Pankanti, and A. Jain, “Fuzzy vault for fingerprints,” in *Proc. Int. Conf. Audio- and Video-Based Biometric Person Authentication (AVBPA)*, ser. LNCS, vol. 3546. Springer, 2005, pp. 310–319.

- [6] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *IEEE Workshop on Privacy Research In Vision*, C. Schmid, S. Soatto, and C. Tomasi, Eds. IEEE Computer Society, 2006, pp. 163–169.
- [7] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance." *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 4, pp. 744–757, 2007.
- [8] P. Mihailescu, A. Munk, and B. Tams, "The fuzzy vault for fingerprints is vulnerable to brute force attack," in *BIOSIG 2009: Biometrics and Electronic Signatures*, ser. LNI, A. Brömme and C. Busch, Eds., vol. 155. Gesellschaft für Informatik, 2009, pp. 43–54.
- [9] R. Plaga, "Biometric keys: Suitable uses and achievable information content," *Int. J. Inf. Secur.*, vol. 8, no. 6, pp. 447–454, 2009.
- [10] J. Merkle, H. Ihmor, U. Korte, M. Niesing, and M. Schwaiger, "Provable security for the fuzzy fingerprint vault," in *Proc. 5th Int. Conf. Internet Monitoring and Protection (ICIMP 2010)*. IEEE Computer Society, 2010, pp. 65–73.
- [11] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data." *SIAM J. Computing*, vol. 38, no. 1, pp. 97–139, 2008.
- [12] K. Nandakumar, "Multibiometric systems: Fusion strategies and template security," Ph.D. dissertation, Michigan State University, 2008.
- [13] C. Watson, M. Garriss, E. Tabassi, C. Wilson, M. McCabe, S. Janet, and K. Ko, *User's Guide to NIST Biometric Image Software (NBIS)*, National Institute of Standards and Technology, 2007.
- [14] Y. Chen, S. Dass, and A. Jain, "Fingerprint quality indices for predicting authentication performance," in *Proc. Audio- and Video-Based Biometric Person Authentication (AVBPA 2005)*, ser. Lecture Notes in Computer Science, T. Kanade, A. K. Jain, and N. K. Ratha, Eds., vol. 3546. Springer, 2005, pp. 160–170.
- [15] M. Liu, X. Jiang, and A. C. Kot, "Fingerprint reference-point detection," *EURASIP J. Appl. Signal Process.*, vol. 2005, pp. 498–509, 2005.
- [16] J. Jeffers and A. Arakala, "Fingerprint alignment for a minutiae-based fuzzy vault," in *IEEE Biometrics Symposium*, 2007, pp. 1–6.
- [17] J. Li, X. Yang, J. Tian, P. Shi, and P. Li, "Topological structure-based alignment for fingerprint fuzzy vault," in *19th International Conference on Pattern Recognition (ICPR 2008)*, 2008, pp. 1–4.
- [18] W. J. Scheirer and T. E. Boulton, "Cracking fuzzy vaults and biometric encryption," in *Proc. IEEE Biometrics Symposium*, 2007, pp. 1–6.
- [19] J. v. z. Gathen and J. Gerhard, *Modern Computer Algebra*, 2nd ed. Cambridge University Press, 2003.
- [20] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the original point set hidden among chaff," in *Proc. ACM Symp. on Information, Computer & Communication Security (ASIACCS)*. ACM, 2006, pp. 182–188.